

(19)

JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **10229401 A**(43) Date of publication of application: **25.08.98**

(51) Int. Cl.

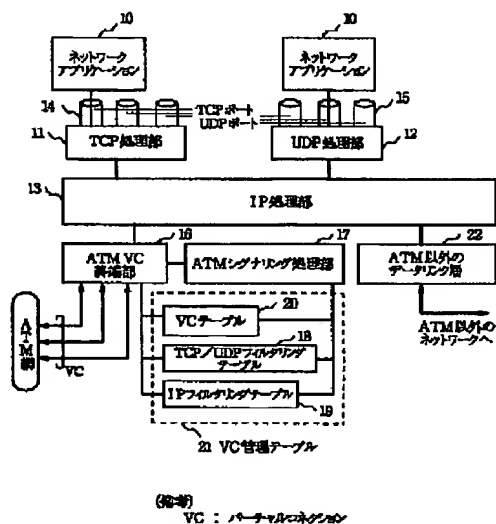
H04L 12/28**H04L 29/04****H04Q 3/00**(21) Application number: **09030436**(71) Applicant: **NEC CORP**(22) Date of filing: **14.02.97**(72) Inventor: **MORI NAOKI****(54) COMMUNICATION SYSTEM USING ATM NETWORK**

(57) Abstract:

PROBLEM TO BE SOLVED: To improve the security of communication by preparing a constitution in which a transmitting IP node reports the IP addresses of both transmitting and receiving nodes, the transport layer protocol to be used and the TCP/IP port number and then the transmission is inhibited for the packet number of the node stored by the transmitting node after the virtual connection has been set.

SOLUTION: A network application 10 selects a specific port of TCP ports 14 and UDP ports 15 and sends a packet to it. An IP-processing part 13 processes an IP layer to give a header to it and sends a packet to an ATM VC termination part 16. The part 16 reads the received packet, a TCP/UDP header and an IP reader and retrieves whether or not a VC has been set. If the setting of the VC is confirmed, the part 16 decides the permission or inhibition for transmission of a packet by making a reference to a VC management table 21. Thus, the security of an IP node is enhanced by previously setting a desired filtering rule for an ATM exchange with regards to security.

COPYRIGHT: (C)1998,JPO



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-229401

(43) 公開日 平成10年(1998) 8月25日

(51) Int.Cl.⁶

識別記号

H 0 4 L 12/28

29/04

H 0 4 Q 3/00

F I

H 0 4 L 11/20

H 0 4 Q 3/00

H 0 4 L 13/00

G

3 0 3 B

審査請求 有 請求項の数 5 O L (全 13 頁)

(21) 出願番号

特願平9-30436

(22) 出願日

平成9年(1997) 2月14日

(71) 出願人 000004237

日本電気株式会社

東京都港区芝五丁目7番1号

(72) 発明者 森 直樹

東京都港区芝五丁目7番1号 日本電気株式会社内

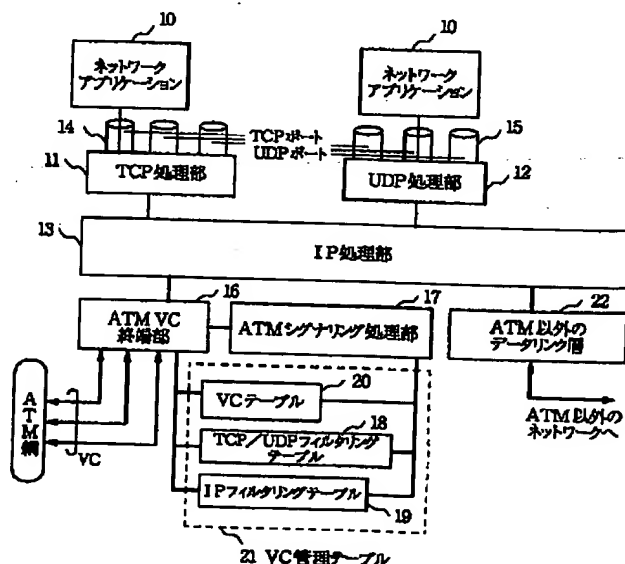
(74) 代理人 弁理士 京本 直樹 (外2名)

(54) 【発明の名称】 ATM網を用いた通信方式

(57) 【要約】

【課題】 通信のセキュリティを向上させる。

【解決手段】 ATMネットワーク中のIPノードが、TCP/IPプロトコルを用いて通信を開始するとき、ATM VCを設定してからパケットを送受信する。送信IPノードはVC設定時に、そのVCを通して送信するTCP/IPパケットの属性を記憶しておくとともに、ネットワークに通知する。ネットワークはその通知をもとに、フィルタリングテーブルを参照してVC設定を許可するか判定する。VC設定後送信IPノードは、VC設定時に記憶した属性を持つTCP/IPパケットのみを、そのVCに対して送信できる。受信IPノードはVC設定時に、そのVCを通して受信してもよいTCP/IPパケットの属性がネットワークより指定される。受信IPノードは、VC設定時に指定された以外の属性を持つTCP/IPパケットは廃棄する。



(備考)

VC : バーチャルコネクション

【特許請求の範囲】

【請求項1】 ATMネットワークインタフェースを持った送信側IPノードがシグナリング手順を起動し、前記送信側IPノードは通信相手の受信側IPノードとの間にバーチャルコネクションを設定して、TCP/IPパケットをATMセル化して通信を行うATM網を用いた通信方式において、

前記送信側IPノードは前記シグナリング手順を起動するときに、前記送信側IPノード内のTCP/IP部分が、送信しようとする前記TCP/IPパケットの前記送信側および前記受信側のIPノードのそれぞれのIPアドレス、トランスポート層のプロトコル、トランスポート層のポート番号を、前記送信側IPノード内のATMシグナリング処理部分に通知し、前記ATMシグナリング処理部は前記通知された値を記憶しておくと共に、ネットワークへの前記シグナリング手順の中で、前記通知された内容を前記ネットワークに対して申告し、いったんそのバーチャルコネクションが設定された後、前記送信側IPノードは記憶しておいた前記送受信それぞれのIPノードの前記IPアドレス、前記トランスポート層プロトコル、前記トランスポート層のポート番号以外を有するTCP/IPパケットを、前記バーチャルコネクションを通して送信することを禁止することを特徴とするATM網を用いた通信方式。

【請求項2】 ATMネットワークインタフェースを持った送信側IPノードがシグナリング手順を起動し、前記送信側IPノードは通信相手の受信側IPノードとの間にバーチャルコネクションを設定して、TCP/IPパケットをATMセル化して通信を行うATM網を用いた通信方式において、
前記バーチャルコネクション設定のためのシグナリング手順を受けたATM交換機内のATMシグナリング処理部は、前記送信側IPノードから申告された前記送信側および前記受信側のそれぞれのIPノードのIPアドレス、トランスポート層プロトコル、トランスポート層ポート番号を読み取り、あらかじめ作成されているバーチャルコネクション設定の許可規則に基づき、そのバーチャルコネクションの設定を許可する場合は設定手順を続行し、許可できない場合にはそのバーチャルコネクションの設定を中止することを特徴とするATM網を用いた通信方式。

【請求項3】 ATMネットワークインタフェースを持った送信側IPノードがシグナリング手順を起動し、前記送信側IPノードは通信相手の受信側IPノードとの間にバーチャルコネクションを設定して、TCP/IPパケットをATMセル化して通信を行う、ATM網を用いた通信方式において、
前記バーチャルコネクション設定のためのシグナリング手順を受けた前記受信側IPノード内のATMシグナリング処理部分は、前記受信側IPノードと前記バーチャ

ルコネクションを設定するときに、前記シグナリング手順の中で通知された前記送信側および前記受信側のそれぞれのIPノードのIPアドレス、トランスポート層プロトコル、トランスポート層ポート番号を記憶しておき、その後前記バーチャルコネクションがいったん設定された、後前記受信側IPノードは、そのバーチャルコネクションを通して、記憶しておいた前記送受信それぞれのIPノードの前記IPアドレス、前記トランスポート層プロトコル、前記トランスポート層ポート番号以外を有するTCP/IPパケットを受信したときは、それを廃棄することを特徴とするATM網を用いた通信方式。

【請求項4】 ATMネットワークインタフェースを持った送信側IPノードがシグナリング手順を起動し、前記送信側IPノードは通信相手の受信側IPノードとの間にバーチャルコネクションを設定して、TCP/IPパケットをATMセル化して通信を行うATM網を用いた通信方式において、

前記送信側および前記受信側のそれぞれのIPノード間にバーチャルコネクションが設定されていて、そこを通して送受信することを許可されているパケットの、前記送受信それぞれのIPアドレス、トランスポート層プロトコル、トランスポート層番号が指定されているときに、既に前記許可されているパケットに加えて、前記送受信それぞれのIPノードが、別の送受信それぞれのIPアドレス、トランスポート層プロトコル、トランスポート層番号を持つパケットを、前記バーチャルコネクションを通して送受信することを許可させる要求をネットワークに通知し、このネットワーク内のATM交換機では、予め設定された規則に基づいて前記要求を許可するかどうか判定し、許可する場合は前記送受信それぞれのIPノードに前記パケットの送受信許可を通知し、許可できない場合には前記送受信それぞれのIPノードに前記パケットの送受信を禁止を通知することを特徴とするATM網を用いた通信方式。

【請求項5】 前記ネットワーク内のATM交換機が、予め設定された規則に基づいて、前記送受信それぞれのIPノードにパケットの送受信許可を通知するときに、要求されたパケットの送受信を許可するのみだけでなく、送受信することが許可される他の1つまたは複数のパケットの、前記送受信それぞれのIPノードの前記IPアドレス、前記トランスポート層プロトコル、前記トランスポート層ポート番号を通知することを特徴とする請求項4記載のATM網を用いた通信方式。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、非同期転送(Asynchronous Transfer Mode; ATM)網を用いた通信方式に関し、特にATM網を用いたTCP/IPプロトコルによるインターネットの構成で

の通信セキュリティを確保する通信方式に関する。

【0002】

【従来の技術】この種の従来のATM網を用いた通信方式では、ネットワーク層にIPプロトコルを、トランスポート層にTCPとUDPプロトコルを用いたTCP/IPネットワークを互いに接続する場合に、これまでルータが用いられてきた。ルータは複数のネットワークインタフェースを持ち、ネットワーク層までの処理を終端する。またトランスポート層の処理一部行うことがある。

【0003】ルータの機能の1つとして、パケットとのフィルタリングによる通信セキュリティの確保がある。あるネットワークの外部にあるIPノードが、ネットワークの内部にあるIPノードと通信するときに、ネットワークの出入口にあるルータを経由する。ルータはパケット内のネットワーク層とトランスポート層のヘッダを読んで、転送を行っている。そのため、そこを通過してよいTCP/IPパケットの送信IPノード・受信IPノードのIPアドレスとTCP/UDPのポート番号を設定し、それに該当しないパケットを廃棄するようになると、ネットワーク内部のIPノードを外部からアクセスできなくなったり、特定のトランスポート層のポートへのアクセスを禁止したりすることができる。これはそれぞれ、ネットワーク層レベルのパケットフィルタリング、トランスポート層レベルのパケットフィルタリングと呼ばれ、通信セキュリティを高めることに有用である。

【0004】尚、OSI階層モデルでの第2層以下にATMを、第3、4層にTCP/IPプロトコルを用いるときの通信方式について、The ATM ForumやIETF (Internet Engineering Task Force) において審議され、ATM Forum 96-0824r9や、draft-ietf-rolc-nhrp-09.txtなどの仕様書が発表されている。これらの仕様の中でのNHRP方式やMPOA方式では、ネットワークの高速化のために、ルータに代わり高速なATM交換機が用いられるようになっている。このようなネットワークでは、シグナリングと呼ばれる制御手順で送受信IPノード間にバーチャルコネクション(VC)を設定した後、そのVCを通して通信を行う。VCに送信されるTCP/UDPパケットは、送信IPノードでセルと呼ばれる固定長の短い単位に分割されてネットワークに送られ、中継ATM交換機をセルのままでスイッチされ、受信IPノードで再びTCP/UDPパケットに組み立てられる。

【0005】

【発明が解決しようとする課題】この従来のATM網を用いた通信方式では、セルの状態でネットワークを配送されるために、従来のルータとは異なり中継のATM交換機では、パケット内のTCP/UDPヘッダ、IPヘ

ッダの読み取りは行われない。そのため、ルータが行うトランスポート層レベル、ネットワーク層レベルでのパケットフィルタリングが出来なくなるという問題点があり、これがセキュリティ上の問題となるという問題点がある。

【0006】本発明の目的は、上記の問題を解決するために、ATM交換機からなるネットワークにおいても、ルータが行っていたパケットフィルタリングの機能を実現することである。

10 【0007】

【課題を解決するための手段】本発明のATM網を用いた通信方式は、ATMネットワークインタフェースを持った送信側IPノードがシグナリング手順を起動し、前記送信側IPノードは通信相手の受信側IPノードとの間にバーチャルコネクションを設定して、TCP/IPパケットをATMセル化して通信を行うATM網を用いた通信方式において、前記送信側IPノードは前記シグナリング手順を起動するときに、前記送信側IPノード内のTCP/IP部分が、送信しようとする前記TCP/IPパケットの前記送信側および前記受信側のIPノードのそれぞれのIPアドレス、トランスポート層のプロトコル、トランスポート層のポート番号を、前記送信側IPノード内のATMシグナリング処理部分に通知し、前記ATMシグナリング処理部は前記通知された値を記憶しておくと共に、ネットワークへの前記シグナリング手順の中で、前記通知された内容を前記ネットワークに対して申告し、いったんそのバーチャルコネクションが設定された後、前記送信側IPノードは記憶していた前記送受信それぞれのIPノードの前記IPアドレス、前記トランスポート層プロトコル、トランスポート層のポート番号以外を有するTCP/IPパケットを、前記バーチャルコネクションを通して送信することを禁止する。

【0008】本発明のATM網を用いた通信方式は、ATMネットワークインタフェースを持った送信側IPノードがシグナリング手順を起動し、前記送信側IPノードは通信相手の受信側IPノードとの間にバーチャルコネクションを設定して、TCP/IPパケットをATMセル化して通信を行うATM網を用いた通信方式において、前記バーチャルコネクション設定のためのシグナリング手順を受けたATM交換機内のATMシグナリング処理部は、前記送信側IPノードから申告された前記送信側および前記受信側のそれぞれのIPノードのIPアドレス、トランスポート層プロトコル、トランスポート層ポート番号を読み取り、あらかじめ作成されているバーチャルコネクション設定の許可規則に基づき、そのバーチャルコネクションの設定を許可する場合は設定手順を続行し、許可できない場合にはそのバーチャルコネクションの設定を中止する。

50 【0009】本発明のATM網を用いた通信方式は、A

TMネットワークインタフェースを持った送信側IPノードがシグナリング手順を起動し、前記送信側IPノードは通信相手の受信側IPノードとの間にバーチャルコネクションを設定して、TCP/IPパケットをATMセル化して通信を行うATM網を用いた通信方式において、前記送信側および前記受信側の送受信それぞれのIPノード間にバーチャルコネクションが設定されていて、そこを通して送受信することを許可されているパケットの、前記送受信それぞれのIPアドレス、トランスポート層プロトコル、トランスポート層番号が指定されているときに、既に前記許可されているパケットに加えて、前記送受信それぞれのIPノードが、別の送受信それぞれのIPアドレス、トランスポート層プロトコル、トランスポート層番号を持つパケットを、前記バーチャルコネクションを通して送受信することを許可させる要求をネットワークに通知し、このネットワーク内のATM交換機では、予め設定された規則に基づいて前記要求を許可するかどうか判定し、許可する場合は前記送受信それぞれのIPノードに前記パケットの送受信許可を通知し、許可できない場合には前記送受信それぞれのIPノードに前記パケットの送受信を禁止を通知し、前記ネットワーク内のATM交換機が、予め設定された規則に基づいて、前記送受信それぞれのIPノードにパケットの送受信許可を通知するときに、要求されたパケットの送受信を許可するのみだけでなく、送受信することが許可される他の1つまたは複数のパケットの、前記送受信それぞれのIPノードの前記IPアドレス、前記トランスポート層プロトコル、前記トランスポート層ポート番号を通知する。

【0010】

【発明の実施の形態】次に、本発明について図面を参照して説明。

【0011】図1は本発明の第1の実施の形態のIPノードにおける、TCP/IPプロトコルとATM通信部に関する機能構成図である。

【0012】尚、本第1の実施の形態においてはVCは単方向であり、IPノード間で双方向の通信を行うときには、異なる方向の2つのVCを独立して設定する。また一つのIPノード内で異なるTCP/UDPポートを用いて、同一の相手IPノードと通信をするときには、別々のVCを使用する構成とする。

【0013】図1に示す本第1の実施の形態において、ネットワークアプリケーション10は、TCP/IPとATMを使用してネットワークを利用するプログラムである。TCP処理部11、UDP処理部12、IP処理部13は、それぞれTCPプロトコル、UDPプロトコル、IPプロトコルに関する通信処理をする機能部である。TCPポート14とUDPポート15は、ネットワークアプリケーション10がTCPプロトコルまたはUDPプロトコルを利用するための通信インタフェースで

あり、ネットワークアプリケーション10は一つのポートを選択する。各ポートには、固有のポート番号が付与されている。ATM VC終端部16は、IP処理部13とATMネットワークとのインタフェースであり、送信時にはIP処理部13から受けたパケットをATMセル化してVCを通してネットワークに送信し、受信方向ではVCを通して送られてきたATMセルをIPパケットに組み立てて、IP処理部13にわたす。ATMシグナリング処理部17は、ATM VC終端部16からの命令や、ネットワークからのシグナリングメッセージの到着により、VCを設定するためのシグナリングの制御・処理をする。TCP/UDPフィルタリングテーブル18とITPフィルタリングテーブル19は、VC設定時に記憶した情報に基づいて、あるVCに送信できるパケットと、VCを通して受信できるパケットを制御するためのものである。TCP/UDPフィルタリングテーブル18は、TCP/UDPポート番号により、IPフィルタリングテーブル19は送受信IPノードのIPアドレスによって上記制御を行う。VCテーブル20は、設定したVCを登録・管理するために用いられる。TCP/UDPフィルタリングテーブル18、IPフィルタリングテーブル19、VCテーブル20を合わせて、VC管理テーブル21と呼ぶ。ATM以外のデータリンク層22は、ATM以外のネットワークとの入出力パケットを制御する機能部である。

【0014】図2は、本第1の実施の形態の送信側IPノードにおける、パケット送信時の手順を示す図である。

【0015】第1の実施の形態では、VCは単方向であるとする。図2において、本IPノードがデータの送信元のときは手順101を行い、ネットワークアプリケーション10がパケットを送信するために、TCPポート14またはUDPポート15の中の特定のポートを選択して、パケットを渡す。次に手順102において、そのパケットを受けたTCP処理部11またはUDP処理部12は、それぞれTCP層、UDP層の処理を行い、パケットヘッダを付加してIP処理部13にそのパケットを渡す。次に手順103-1で、IP処理部13はIP層の処理をしてヘッダを付与し、ATM VC終端部16にパケットを渡す。本IPノードがATM以外のネットワークから受けたデータをATM網に中継するときは、手順103-2を行い、ATM以外のデータリンク層22から受けたパケットをIP処理し、ATM VC終端部16にパケットを渡す。以後の処理は、手順103-1を行ったときも、手順103-2を行ったときも共通である。

【0016】次に手順104においてATM VC終端部16は、渡されたパケットとTCP/UDPヘッダ、IPヘッダを読んだ後、それらの送受信IPノードのTCP/UDPポート間にVCが既に存在するかどうか検

索する。

【0017】VCが設定されていないときは、シグナリング手順を起動するために手順105を行い、ATMシグナリング処理部17にVC設定を依頼する。この時に、送信しようとするパケットの送受信IPノードのIPアドレスとTCP/UDPのポート番号を、ATMシグナリング処理部に通知する。このときオプションとして、ネットワークアプリケーション10の種別(識別子)を通知することも可能である。次に手順106を行い、ATMシグナリング処理部17は受信IPノードへのVC設定要求のシグナリングをネットワークに対して開始する。この時に、送受信IPノードのATMアドレスに加えて、IPアドレス、TCP/UDPポート番号をネットワークに通知する。またオプションとして、ネットワークアプリケーション10の種別(識別子)を通知することもある。受信IPノード側とネットワークにおいて上記VCの設定が成功すると、ネットワークから送信IPノードに通知される。その後手順108を行い、設定したVCをIP処理部13の出力として、VC管理テーブル21に、送信を許可されたパケットの送受信IPノードのIPアドレスとTCP/UDPのポート番号、オプションのネットワークアプリケーション10の種別(識別子)と共に登録する。そして手順109で、上記VCを使用して受信IPノードにパケットを送信する。

【0018】図3は、本第1の実施の形態のIPノードにおけるVC管理テーブル21の内容の例を示す図である。

【0019】図3において、列31は、VPI=0、VCI=103のVCは、IPアドレスが133.207.36.112のIPノード内のTCP8010番のポートを送信側とし、IPアドレスが133.207.38.123のIPノード内のTCP25番から100番のポートを受信側としていることを表す。列32は、VPI=2、VCI=129のVCは、IPアドレスが133.207.38.222のIPノード内のUDP517番のポートを送信側とし、IPアドレスが133.207.36.111とIPノード内のUDP8080番のポートを受信側としていることを表す。またそのVCを使用しているネットワークアプリケーション10の種別(識別子)が、送信側161・受信側161であることを表す。

【0020】手順104において既にVCが設定されているときは手順110を行い、ATM VC終端部16は、VC管理テーブル21を参照して、そのVCを通してパケットを受信IPノードに送ってよいか判定する。オプションとして、ネットワークアプリケーション10の種別によっても、パケット送信の許可・不許可を判定することも可能である。送信が許可されているとき、ATM VC終端部16は手順111を行い、パケットを

そのVCを通して送信する。送信が許可されていないときは、手順112を行いパケットを廃棄する。

【0021】図4は、本第1の実施の形態におけるネットワーク内のATM交換機を示す機能構成図である。

【0022】図4において、スイッチハードウェア51は、設定されたVCにしたがってATMセルをスイッチングするハードウェア部である。シグナリング処理部52は、受信したシグナリングメッセージを処理する部分である。スイッチハードウェア制御部53は、シグナリング処理部52の命令に従って、VCをスイッチハードウェア21に設定する部分である。交換機フィルタリングテーブル54は、送受信IPノードのIPアドレス、トランスポート層プロトコル、TCP/UDPポート番号により、その交換機を経由して設定できるVCに関して制限を加える部分である。オプションとして、ネットワークアプリケーション10の種別によってVC設定を制限する機能部を追加することも可能である。

【0023】図5は、本第1の実施の形態における、ATM交換機がVC設定要求のシグナルメッセージを受けた時の処理手順を示す図である。

【0024】図5において、手順201で、隣接するATM交換機またはIPノードからシグナリングメッセージを、シグナリング処理部52が受信する。そして手順202で、シグナリング処理部52は、受けたシグナリングメッセージ中の受信IPノードのATMアドレスから出力回線を決定する。次に手順203で、上記シグナリングメッセージに含まれる送受信IPノードのIPアドレスとTCP/UDPポート番号を読み、交換機フィルタリングテーブル54を参照して、入力側の回線と出力側の回線にVCを設定してよいか判定する。オプションとして、ネットワークアプリケーション10の種別によっても、判定を行うことは可能である。

【0025】図6は本第1の実施の形態における交換機フィルタリングテーブル54の内容の例を示す図である。

【0026】図6において列31は、IPアドレスが133.207.36.111のIPノードの任意のポートと、IPアドレスが133.207.38.123のIPノードのTCP25番から100番ポートとの間にVCを設定することを許可することを表す。列32は、IPアドレスが133.207.36.222のIPノードのUDP517番ポートと、IPアドレスが133.207.37.111のIPノードのUDP8080番ポートとの間にVCを設定することを許可することを表す。列33は、IPアドレスが133.207.36.0のネットワークにある全てのIPノードのTCP20または21番ポートとの間に、種別が161であるネットワークアプリケーション使用するためのVCを設定することを許可することを表す。列34は、IPアドレスが133.207.36.0のネットワークにある

全てのIPノードの任意のポートと、IPアドレスが133.207.0.0以外のネットワークにある全てのIPノードの任意のポートとの間にVCを設定することを禁止することを表す。

【0027】手順203の結果、VCの設定が許可された場合には手順204を実行し、VC設定のシグナリングメッセージを、送信するパケットの送受信IPノードのIPアドレスとTCP/UDPのポート番号と共に出力側の回線を介して、次段のATM交換機またはIPノードに送信する。この時、ネットワークアプリケーション10の種別や、このVCを通して送信することが許可される他のパケットの、IPアドレス、TCP/UDPポート番号を、上記シグナリングメッセージに含ませることも可能である。VCと設定が許可されない場合には手順205を実行し、VCの設定を中断して前段の交換機またはIPノードにそれを通知する。

【0028】図7は、本第1の実施の形態におけるVC設定要求のシグナルメッセージを受けた時の、IPノードの手順を示す図である。

【0029】図7において、手順301で、隣接のATM交換機からVC設定要求のシグナリングメッセージを、ATM VC終端部16を通して、ATMシグナリング部17が受信する。次に手順302で、ATMシグナリング部17はシグナリング処理を行い、ATM VC終端部16にVCを設定し、入力としてIP処理部13に接続する。そして手順303で、ATMシグナリング処理部17は、設定したVCを、そのVCを通して送受信することが許可されたパケットの送受信IPノードのTCP/UDPポート番号、IPアドレスと、オプションのネットワークアプリケーション10の種別と共にVC管理テーブル21に登録する。

【0030】図8は、本第1の実施の形態におけるネットワークからデータを受信したときのIPノードでの手順を示す図である。

【0031】図8において、手順401において、ATM VC終端部16は、受信したデータセルをからパケットを組み立てる。次に手順402において、ATM VC終端部16は、組み立てたパケットのIPヘッダとTCP/UDPヘッダから、送受信IPノードのTCP/UDPポート番号とIPアドレスを読み取り、VC管理テーブル21を参照して、受信パケットをIP処理部13に渡してもよいか判定する。オプションとして、ネットワークアプリケーションの識別子も、判定の基準に使用する。許可された場合には手順404として、ATM VC終端部16は上記パケットをIP処理部13に渡す。許可されない場合には手順405として、ATM VC終端部16は、上記パケットを廃棄する。

【0032】次に、本発明の第2の実施の形態について図面を参照して説明する。

【0033】この第2の実施の形態では双方向のVCを

用い、通信を開始するときに、IPノード間に同じVP I/VC Iで異なる方向のVCを同時に設定するような構成をとる。また一つのIPノード内の異なるTCP/UDPポートを用いて、同一の相手IPノードと通信をするときには、同一のVCを使用する構成とする。IPノードにおけるTCP/IPプロトコルとATM通信に関する機能構成図と、ATM交換機を示す機能構成図は第1の実施の形態と同じで、それぞれ図1と図4とで表される。

10 【0034】図9は、本第2の実施の形態の送信側IPノードにおけるパケット送信時の手順を示す図である。

【0035】図9において、手順501、502、503-1、503-2、504は、第1の実施の形態1の手順101、102、103-1、103-2、104とそれぞれ同じである。手順504の結果、受信IPノードへのVCが設定されていないときには、手順505、506、507、508、509を行う。これらの手順は、第1の実施の形態1の手順105、106、107、108、109と同じである。手順504の結果、送受信IPノード間の送受信TCP/UDPポート間にVCが既に設定されている場合は、手順510を行い、その後手順511または512を行う。手順510、511、512は、第1の実施の形態1の手順110、111、112と同じである。手順504の結果、送受信IPノード内のこれから通信で使用するTCP/UDPポート間以外にVCが設定されている場合は、手順513を行い、既に設定されたVCに、別のTCP/IPの属性を持つパケットを通すための手順を開始する。手順513でATM VC終端部16は、ATMシグナリング制御部17に、送受信IPノードのIPアドレス、送受信IPノードのTCP/UDPポート番号を通知し、VCに送信できるパケットの追加を依頼する。次に手順514で、ATMシグナリング制御部17は、受信IPノードのIPアドレスからATMアドレスを検索する。次に手順515で、受信IPノードへのVCに送受信できるパケット追加要求のシグナリングを、ネットワークに対して開始する。この時に、送受信IPノードのATMアドレスに加えて、IPアドレス、TCP/UDPポート番号をネットワークに通知する。またオプションとして、ネットワークアプリケーション10の種別（識別子）を通知することも可能である。受信IPノード側とネットワークにおいて上記送受信パケットの追加要求が成功すると、ネットワークから送信IPノードに通知される。その後手順516を行い、VC管理テーブル21内で、新たに追加した送受信IPノードのTCP/UDPのポート番号を、上記VCに追加登録する。そして手順517で、上記VCを使用して受信IPノードにパケットを送信する。

50 【0036】図10は、本第2の実施の形態におけるATM交換機が、VCに送信できるパケットの追加依頼の

シグナリングメッセージを受けた時の処理手順を示す図である。

【0037】図10において、手順601で、隣接するATM交換機またはIPノードからシグナリングメッセージを、シグナリング処理部52が受信する。次に手順602で、上記シグナリングメッセージに含まれる送受信IPノードのIPアドレスとTCP/UDPポート番号を読み、交換機フィルタリングテーブル54を参照して、新たなパケットと送受信を許可してもよいか判定する。オプションとして、ネットワークアプリケーション10の種別によっても、判定を行うことは可能である。手順602の結果、許可された場合には手順603を実行し、既存のVCに対し新たなパケットの送受信の許可を要求するシグナリングメッセージを出力側の回線を介して、次段のATM交換機またはIPノードに送信する。許可されない場合には手順604を実行し、追加処理を中断して前段の交換機またはIPノードにそれを通知する。

【0038】図11は、本第2の実施の形態における既存のVCに新たなパケットの送受信の許可を要求するシグナリングメッセージを受けた時の、IPノードの手順を示す図である。

【0039】図11において、手順701で、隣接のATM交換機から許可要求のシグナリングメッセージを、ATM VC終端部16を通して、ATMシグナリング部17が受信する。次に手順702で、ATMシグナリング処理部17は、VC管理テーブル21内で、新たに追加した送受信IPノードのTCP/UDPのポート番号を、上記VCに追加登録する。

【0040】

【発明の効果】以上説明したように本発明は、中継のATM交換機に従来のルータ同様のトランスポートレイヤとネットワークレイヤの情報によってフィルタリング規則を記述しておき、シグナリングによるVC設定時に、送信IPノードが送受信それぞれのノードのIPアドレス、使用するトランスポート層プロトコル(TCPまたはUDP)、TCP/UDPポート番号を申告し、それらがフィルタリング規則で禁止されていないかを中継のATM交換機で検査することでシグナリング時のフィルタリングを行い、VC設定後はその申告通りのパケットを送っているかを検査することでデータ転送時のフィルタリングを行い、受信IPノードでは、シグナリングによるVC設定時に、送信IPノードからネットワークを通して申告された送受信IPノードのIPアドレス、トランスポート層プロトコル、TCP/UDPのポート番号を記憶し、VC設定後はその記憶した属性以外のパケットを廃棄することより、TCP/UDPパケット毎にATM交換機でTCP/UDPヘッダとIPヘッダを確認しなくても、IPノードでそれらのヘッダを読んで、IPアドレスとTCP/UDPポート番号によるフィル

タリングを実現することでき、また、このフィルタリング規則は、各IPノードの個々の設定とは無関係であり、中継のATM交換機で設定された規則によって定められ、そのため、中継のATM交換機のフィルタリング規則をセキュリティ上望ましい設定にておくと、そのATM交換機の下流側にある全てのIPノードのセキュリティが向上することになるという効果がある。

【図面の簡単な説明】

【図1】本発明の第1の実施の形態のIPノードにおける、TCP/IPプロトコルとATM通信部に関する機能構成図である。

【図2】本第1の実施の形態の送信側IPノードにおける、パケット送信時の手順を示す図である。

【図3】本第1の実施の形態のIPノードにおけるVC管理テーブル21の例を示す図である。

【図4】本第1と実施の形態におけるATM交換機を示す機能構成図である。

【図5】本第1の実施の形態における、ATM交換機がシグナリングメッセージを受けた時の処理手順を示す図である。

【図6】本第1の実施形態におけるATM交換機のフィルタリングテーブル54の例を示す図である。

【図7】本第1の実施の形態における、VC設定要求のシグナリングメッセージを受けた時のIPノードでの手順を示す図である。

【図8】本第1の実施の形態における、ネットワークからデータセルを受信したときのIPノードでの手順を示す図である。

【図9】本発明の第2の実施の形態の送信側IPノードにおける、パケット送信時の手順を示す図である。

【図10】本第2の実施の形態における、ATM交換機がシグナリングメッセージを受けた時の処理手順を示す図である。

【図11】本第2の実施の形態における、VC設定要求のシグナリングメッセージを受けた時のIPノードでの手順を示す図である。

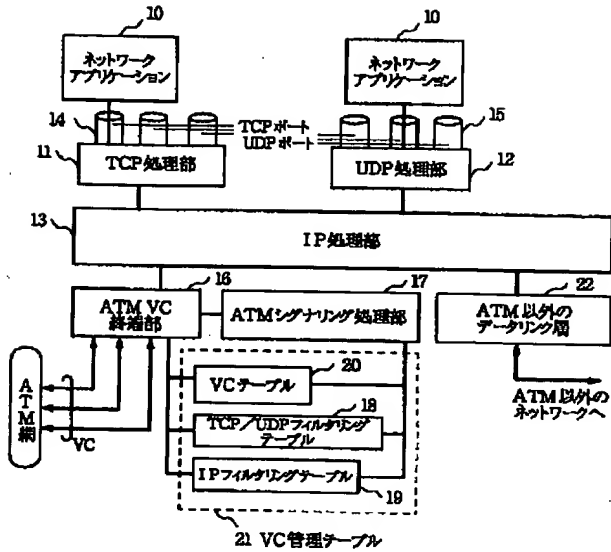
【符号の説明】

- 10 ネットワークアプリケーション
- 11 TCP処理部
- 12 UDP処理部
- 13 IP処理部
- 14 TCPポート
- 15 UDPポート
- 16 ATM VC終端部
- 17 ATMシグナリング処理部
- 18 TCP/UDPフィルタリングテーブル
- 19 IPフィルタリングテーブル
- 20 VCテーブル
- 22 ATM以外のデータリング層
- 51 スイッチハードウェア

- 13
52 シグナリング処理部
53 スイッチハードウェア制御部

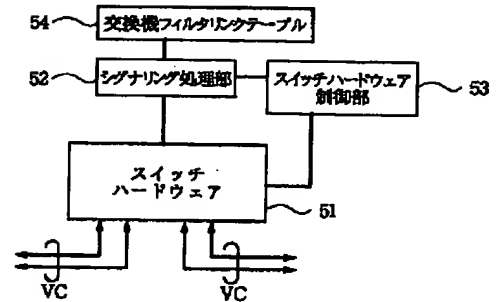
- 54 交換機フィルタリングテーブル

【図1】



(備考)
VC: パーチャルコネクション

【図4】



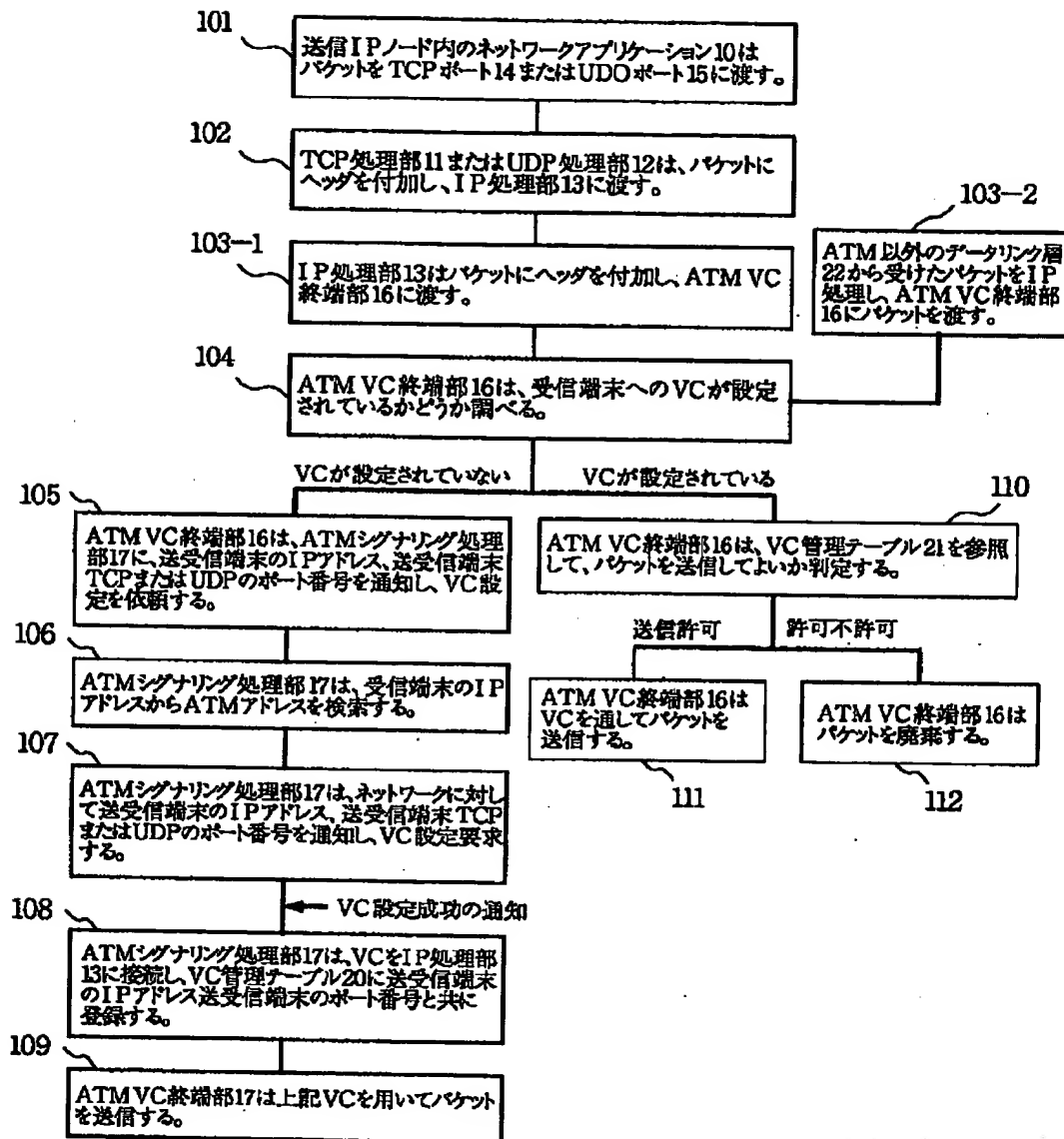
【図3】

	VPI/ VCI	送信端側の IPアドレス	送信端側の TCP/UDPポート番号	受信端側の IPアドレス	受信端側の TCP/UDPポート番号	ネットワーク アプリケーション 識別子
31	0/103	133.207.36.112	8010/TCP	133.207.38.123	25-100/TCP	指定なし
32	2/129	133.207.36.222	517/UDP	133.207.36.111	8080/UDP	161/161

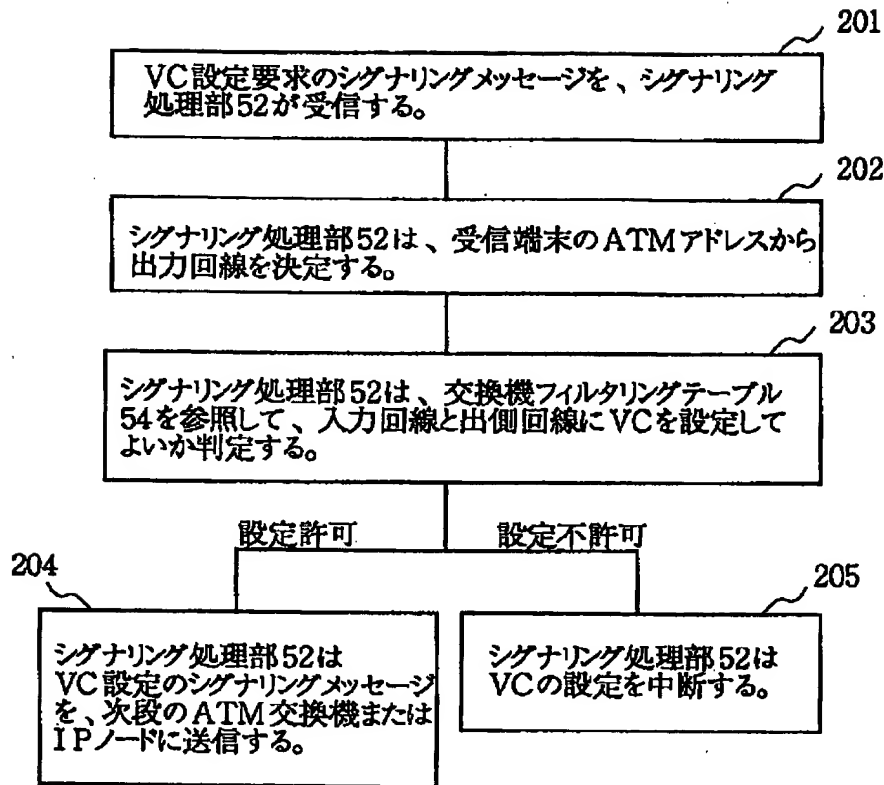
【図6】

	送信端側の IPアドレス	送信端側の TCP/UDPポート番号	受信端側の IPアドレス	受信端側の TCP/UDPポート番号	ネットワーク アプリケーション 識別子	許可 不許可
31	133.207.36.111	指定なし	133.207.38.123	25-100/TCP	指定なし	許可
32	133.207.36.222	517/UDP	133.207.37.111	8080/UDP	指定なし	許可
33	133.207.36.0	指定なし	133.207.38.0	20.21/TCP	161/161	許可
34	133.207.36.0	指定なし	133.207.0.0以外	指定なし	指定なし	不許可

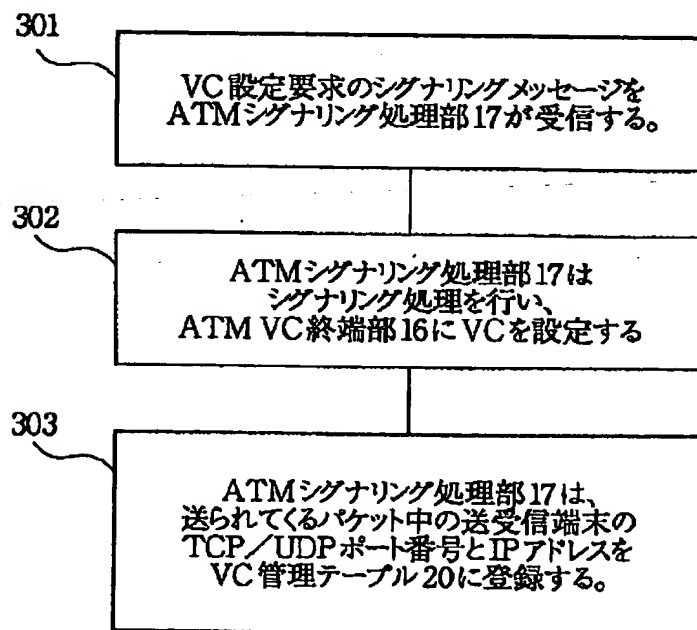
【図2】



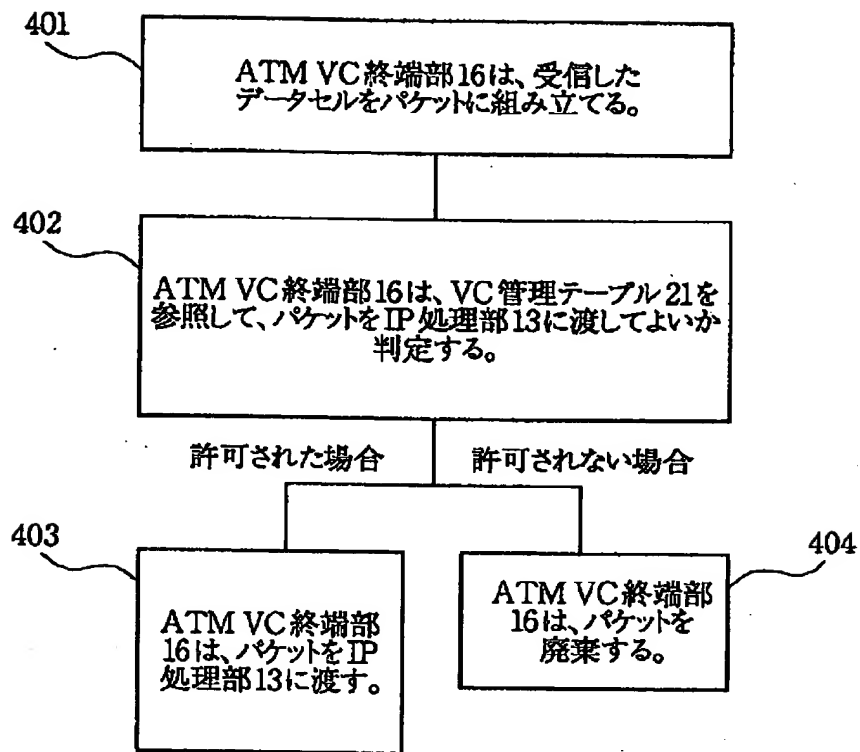
【図 5】



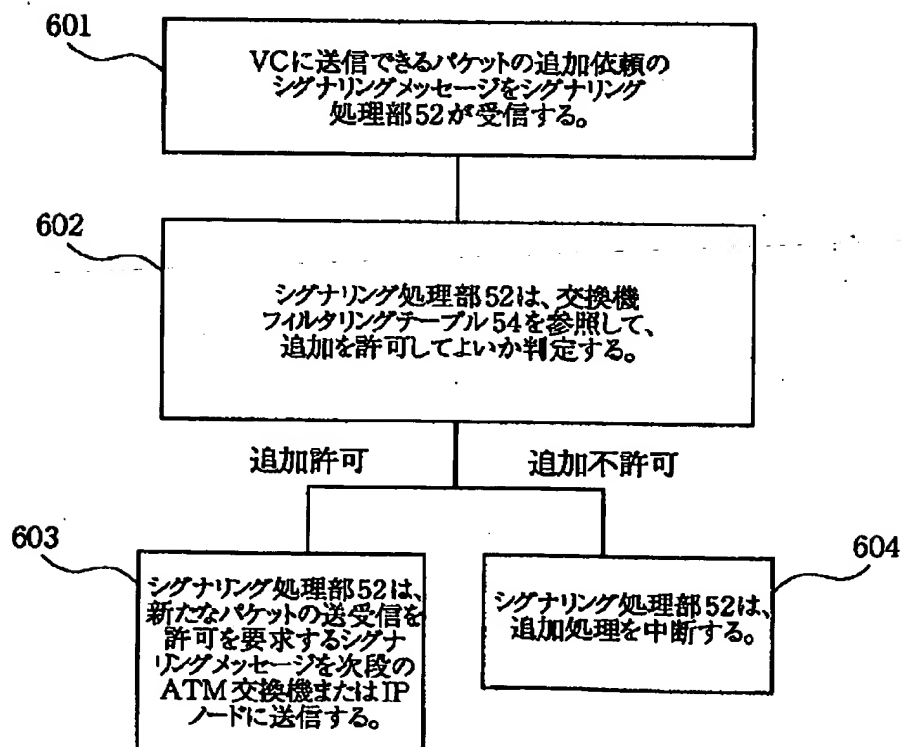
【図 7】



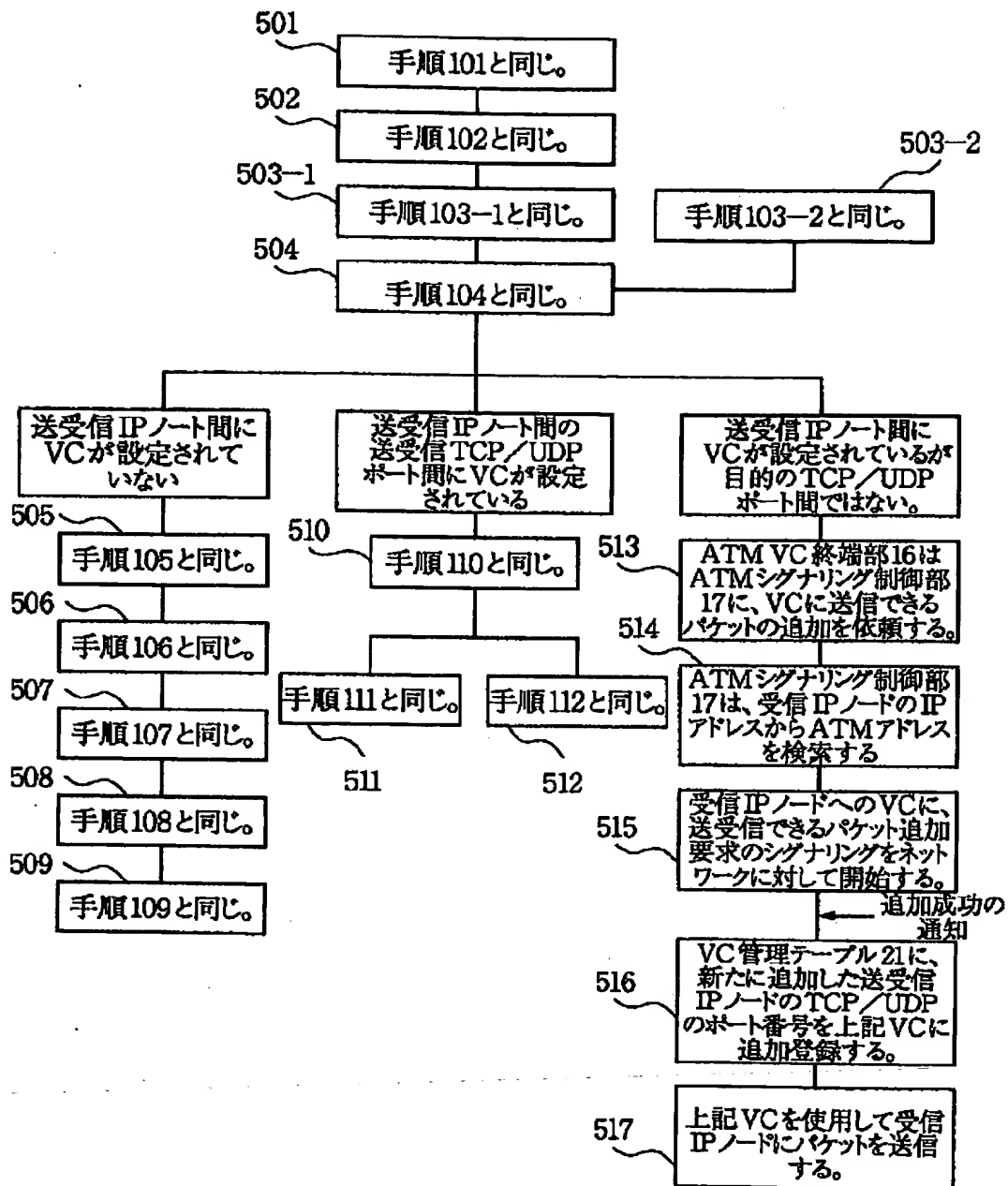
【図 8】



【図 10】



【図 9】



【図11】

